Defense Methods against VoIP and Video Hacking Attacks in Enterprise Networks

Stefan Hofbauer [1], *Kristian Beckers* [2], *Gerald Quirchmayr* [3,4]

Amadeus Data Processing GmbH, Voice, Video & Unified Communications Department, Germany [1]
Technical University Munich, Faculty of Computer Science, Germany [2]
University of Vienna, Multimedia Information Systems Research Group, Austria[3]
University of South Australia, School of Computer and Information Securit, Australia[4]

Abstract— **Theoretical threats against VoIP systems have been elicited and analyzed in the past. Almost a decade after the hype around VoIP security has passed and only few researchers still work in this field, it is time to revisit the topic from a practitioner's perspective. We provide insights about existing VoIP attacks on enterprise networks and illustrate possible countermeasures against them. The threat against VoIP infrastructures is very real, so the protection of companies' systems is of the utmost importance to sustain modern telephone and video communication infrastructures.**

Keywords—threat analysis, Voice-over-IP security, Video-over-IP security, attack prevention

I. Introduction

Telecommunication is increasingly relying on Voice-over-IP technology for the last decade. The topic has been investigated by numerous researchers [1],[2],[3] and a significant number of vulnerabilities in these systems has been identified [4],[5],[6]. However, VoIP systems are still frequently attacked and the proposed solutions often require a fundamental change of the telecommunication infrastructure [1],[3]. In some cases researchers even limit themselves to the publication of possible threats.

In order to address the problem, we require a deeper understanding of current VoIP attacks from a practitioner perspective. Awareness is needed, of affordable solutions for smaller businesses that do not require a fundamental change of the telecommunication systems of a company.

Moreover, today's communications diversify in the amount of services used in such telecommunication infrastructures. Companies combine video communication, chat, and other multiple services using the same infrastructure. Thus, a successful attack on this infrastructure scales to all of these services, and often happens on the border between networks (LAN and WAN). A threat analysis has to consider the complexity of all such systems in order not to miss an important attack vector.

Our contribution is to update current VoIP security assessments and solutions that include scenarios with a diversity of services, particularly video. We show basic architectures of these scenarios and provide threat analysis. We present how the attack surface has increased and provide a set of simple mechanisms for protecting enterprise networks against attack. This paper presents a best practice approach against common attackers in the world. We exclude the almighty attacker used in many theoretical works. The aim of this paper is to provide an analysis from practitioners, for practitioners, and a best practice overview of solutions to mitigate these threats.

Companies widely use communication and collaboration technology (voice, video, web-conferencing, instant messaging, presence status and screen sharing) on premise, from the cloud, or as a hybrid solution. The spread of these technologies, means companies are more vulnerable to attacks, especially against voice and video endpoints (software and hardware clients), as well as infrastructure. Sensitive information exchanged on the communication channel is an incentive for many hackers and for industrial espionage. If a company wants to compete and not lose important information, they need to have the knowledge to secure their environment. Companies are often supported by individual consultants or IT security companies. They have a thorough knowledge of current and historical attacks, to include attack and defense mechanisms with strategies to define a company-wide security concept. The voice and video media data has to be encrypted using client certificates and a company PKI infrastructure. It is not enough to secure the video traffic alone, but also the voice traffic.

Our paper is structured as follows. We provide an overview of common enterprise VoIP and Video architectures in Sect. 2 and an overview of security threats in Sect. 3. Additionally, Section 4 describes defense mechanisms against these threats. We distinguish our work from related approaches in the field and conclude with directions for future research in Sect. 6.

II. ENTERPRISE VOIP AND VIDEO ARCHITECTURES

The VoIP architecture, presented in Fig. 1 consists of several Call manager clusters, a voicemail system and a SME (Session Manager Edition) cluster together with a SBC (Session Border Controller) connected to other SIP providers. The Call manager cluster in our example consists of one publisher and two subscribers. On the subscriber, the IP phones are registering and CTI connections are opened. The publisher houses the read/write copy of the telephony database. The Call manager has all the phone configuration. This consists of the phones (hard-phones and soft-phones), analog devices, SIP third party devices, route pattern, translation pattern, hunt groups, pickup groups, media translation groups, gateways and end user information . The SME holds all the SIP trunks as inter cluster trunks between the Call manager clusters as routing information.

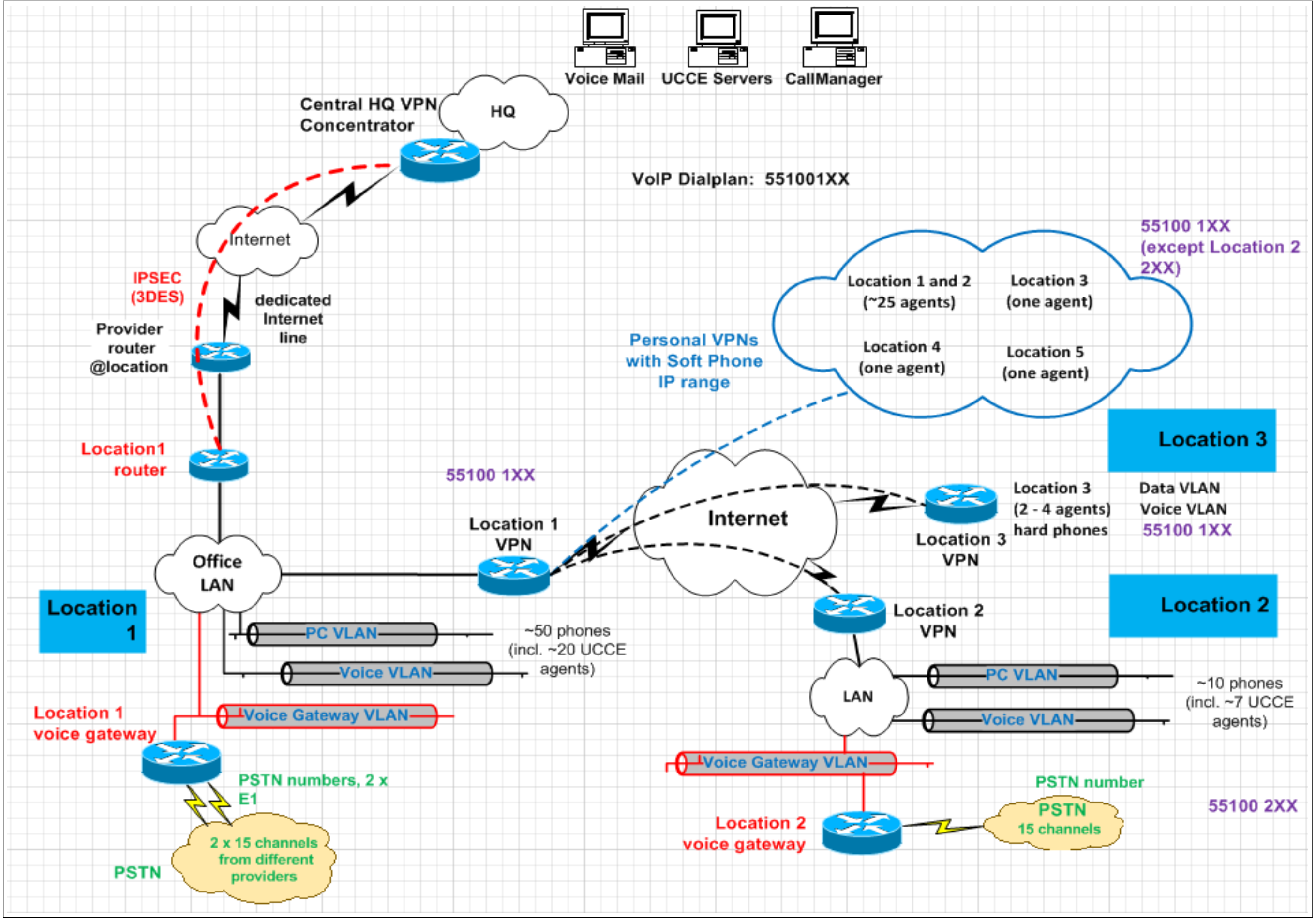

Figure 1: Typical VoIP enterprise architecture

SIP trunks to phone providers and the video architecture, especially VCS (Video Communication Server) and MCU (Media Conferencing Unit). The Call managers are clustered for redundancy reasons with different tasks (publisher and subscriber), CTI (Computer Telephony Integration) Route points and CTI ports. It is recommended to virtualize the Call manager on compliant vendor server hardware. The company VoIP dial plan makes it convenient for employees to dial an eight digit number to reach another site. This model can be reproduced many times, so it scales very well within a company.

The video architecture, presented in Fig. 2 consists of the following components:

VCS-C (Control) cluster, VCS-E (Expressway) cluster, MCUs, ISDN (Integrated Services Digital Network) gateway, Telepresence Content Server, TMS (Telepresence Management Server) server, TMS-XE (Telepresence Management Server Extension for Microsoft Exchange) server, Prime Collaboration Manager and the WebEx enabled Telepresence Integration using the company’s Email server as scheduling platform.

The VCS-C cluster is the gatekeeper for internal registrations of video hardware endpoints, and the video software solution (Jabber Video for Telepresence) within the enterprise network. The VCS-E cluster is the gatekeeper for external registrations of video hardware endpoints, and the video software solution outside the enterprise network (working remotely from home, or different network or from a hotel). The VCS-C and VCS-E servers are clustered, and preferably virtualized for redundancy reasons. The ISDN gateway supports ISDN audio dial-in connections for internal and external customers, who do not support SIP (Session Initiation Protocol). On the Telepresence content server several meeting recordings are stored and archived. This solution allows record and playback meeting for training purposes, and for participants who cannot join or are living in a different time-zone.

an integration. These include a dial-plan structure, URI (Uniform Resource Identifier) dialing and support, Call manager side (correct Call manager release version). Additionally protocol definition, introduction of conductor per location area and security requirements (encryption of audio and video), encryption and use of certificates on hard and soft devices. The integration between audio and video can also be seen at Jabber for Windows / Android / IPhone, where it is possible to access video meeting spots configured on the MCU. The Jabber client is an all in one client having audio, video, screen sharing, web conferencing, and presence and chat capabilities. This is achieved either as on premise, cloud or hybrid solution.

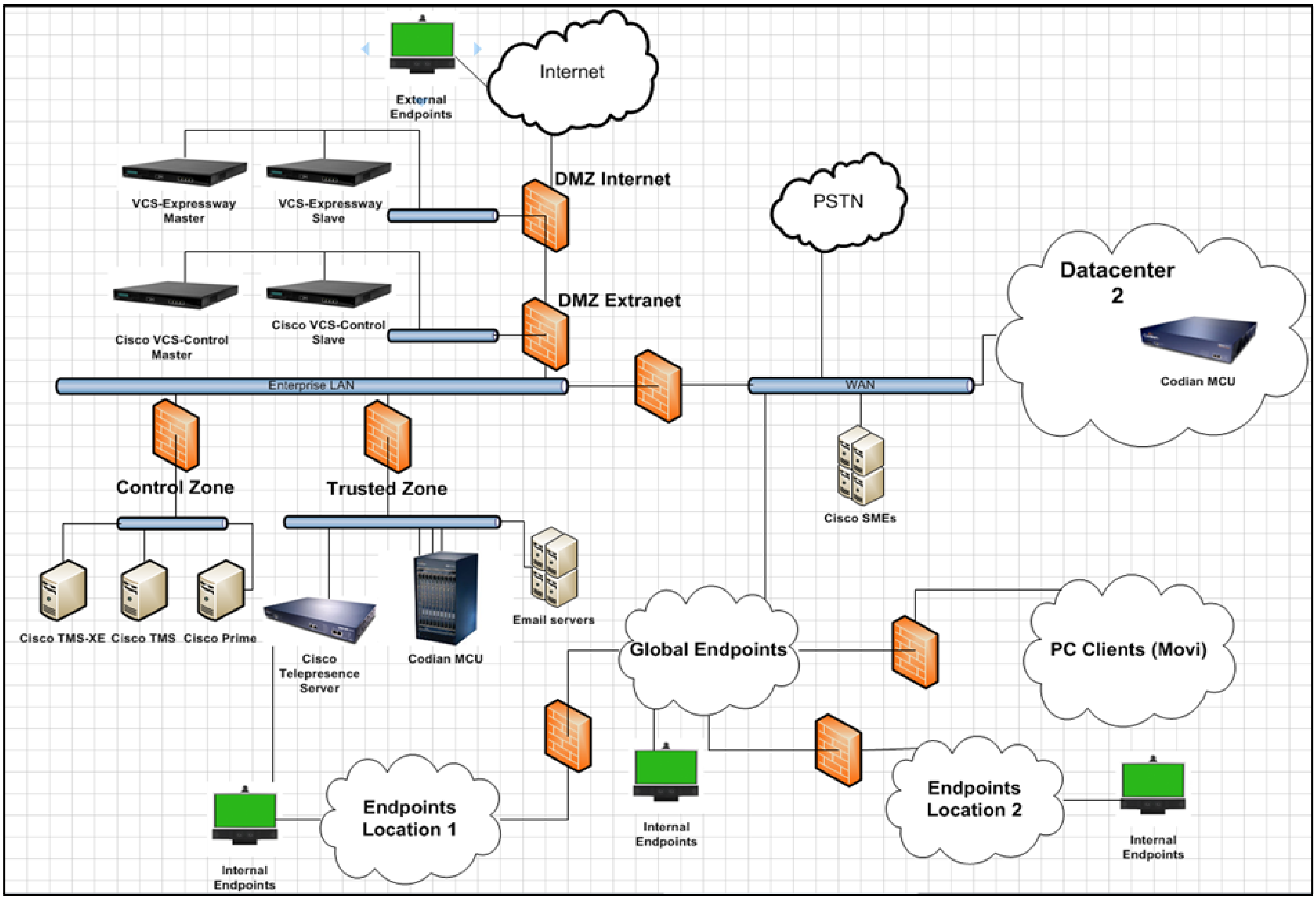

Figure 2: Typical Video enterprise architecture

Finally, the goal is to integrate VoIP and video into one infrastructure. It means that video endpoints and software video clients register on Call manager instead of VCS-C. The media power of the MCU is still needed as DSP resources for conferencing and audio/video mixing of different resolutions and audio/video codecs. There are some prerequisites for such

III. THREAT TAXONOMY

The following threats exist in enterprise networks:

- Using non-secured SIP ports with no authentication in place
- open SIP ports

The problem with open SIP ports is that they can easily be used to register an endpoint on a PBX (Private Branch Exchange) or a VCS-E server. This can occur when there is no authentication in place or where every endpoint, (internal or external) are treated as authenticated. To have only one security zone, without subzones is a security risk. As soon as an endpoint is registered to the gatekeeper (VCS-E or PBX), a rouge endpoint can place outside calls using the outside dial code and thus generate costs leading to toll-fraud. Dependent on the number of free channels, endpoints in use, and time till the attack discovery, thousands of EUR can be exploited and harm the attacked company.

Fig. 3 is an example of a typical integrated VoIP and video enterprise architecture, where video endpoints register on the PBX instead of the VCS-C/E and shall present the different network borders in such an environment. Typically attacks happen between the border of networks and border of technologies.

- Using old, expired certificates or initial certificates issued by the vendor
- expired certificates

Certificates issued by the vendor are not signed and trusted by a public CA (Certificate Authority), like Verisign, Komodo or Thawte. The problem with old, expired certificates is that they can disrupt the services running on these machines.

Two kinds of certificates are in use. Firstly, internal company There are two kind of certificates in use. Firstly, internal company certificates used within the enterprise LAN and signed by the company CA certificates. Secondly external, outside facing WAN servers and services using a public, Internet reachable certificate signed by a public CA.

When a company interacts with other companies or wishes to provide its services to employees using VPN or Internet connection, they require an external entry point (VCS-Expressway or Collaboration Edge) to connect from external

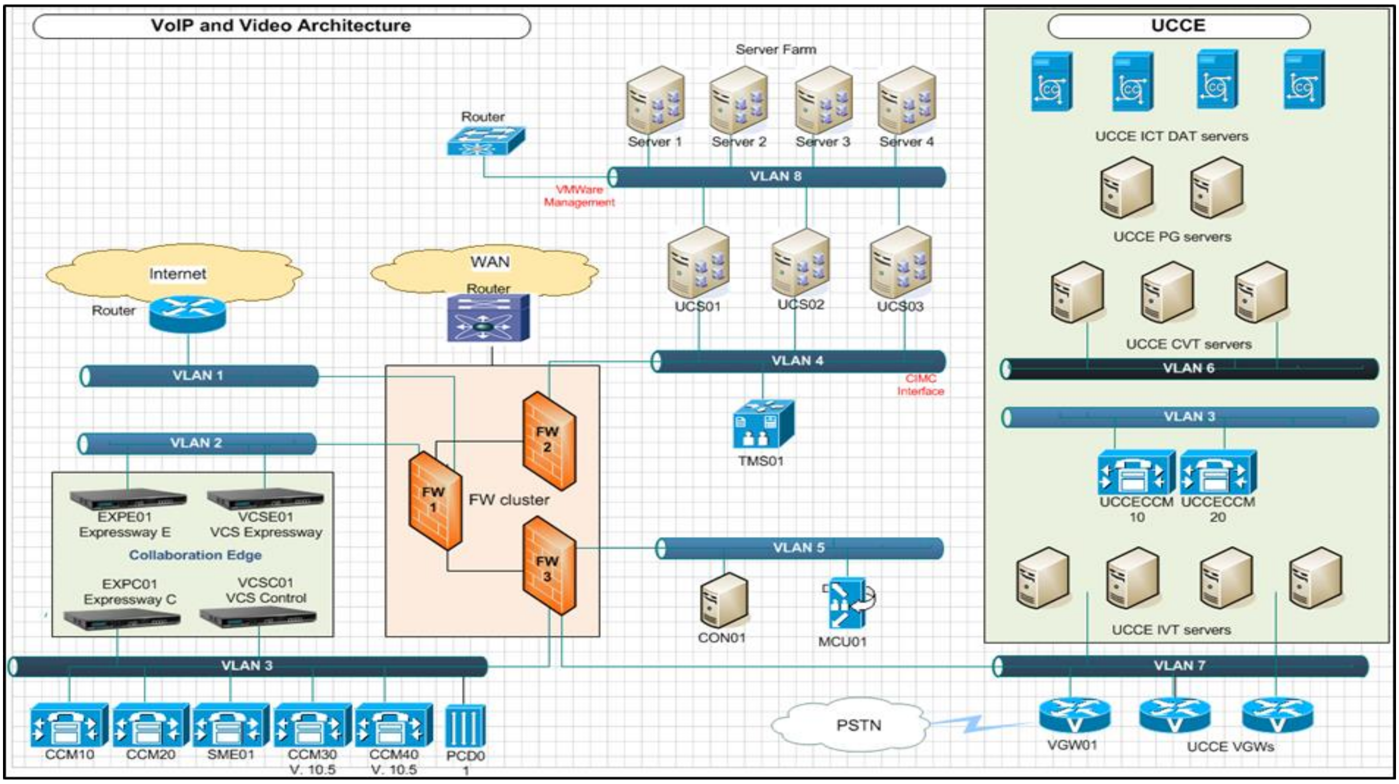

Figure 3: Typical integrated VoIP and Video enterprise architecture

to internal servers. It is advisable to use a multi-layered security approach with both an external and internal firewall DMZ. An attacker has to compromise several security devices to reach the LAN and act as an insider. The collaboration edge solution is also the entry point for external devices to internal services. An example of this is using internal phone services on a mobile device.

- Using non-secure certificates, where the private key can easily be forged - private key forgery

With forged certificates, it is possible to redirect client requests to a different destination. For example a phishing site, which looks similar to the original site, and where credentials are requested and stored in a database to further compromise internal systems. These then have knowledge of internal accounts. Another important point is to have internal and external DNS-A and DNS-SRV records in place for the video architecture. DNS names are also needed for the cluster functionality of the gatekeepers (VCS-C and VCS-E). Be sure to use latest encryption algorithms on the certificates showing compliancy with security policy and Internet browser technology.

- DDOS attacks (via SNMP read community public, root access with default credentials, and using non-secure protocols like HTTP instead of HTTPS)

Having a SNMP read community with the default community (called public) with no credentials makes it easy for attackers to gather more information about the attacked device. The information ranges from vendor information to name and number of interfaces, IP addresses, network port speed and duplex settings. Furthermore, using old firmware with an enabled root account plus vendor default credentials makes it possible for an attacker to gain root access to an endpoint. With root access, an attacker has access to sensitive information (voice and video conversations), can change account credentials and manipulate enterprise devices. Devices running non-secure protocols like HTTP or FTP within an enterprise network enables easier access for attackers to company equipment, because they are not secure and can easily be hacked.

- Public reachable endpoints having the SIP port open for inbound calls - ghost calls

It appears that the codec is calling itself automatically. Placing a codec on a public IP will cause calls from SIP scanners.

These scanners (e.g. SipVicious) are used to detect possibilities for exploiting PSTN trunks. To avoid this, perform the following two configuration changes on the video endpoint: xConfiguration SIP ListenPort: Off ; xConfiguration SIP Profile 1 Outbound: On. Disabling ListenPort stops the endpoint from listening on port 5060/5061 TCP/UDP (SIP). Enabling outbound means all incoming and outgoing calls will re-use the connection open from the endpoint to the VCS from the initial SIP REGISTER message. An example of a ghost call is 1001@192.168.0.2 (extension@IP-address).

- Using old technology (analog gateways, analog telephone adapter, ISDN gateway) - outdated technology

Outdated technology is prone to attacks because the firmware running on its devices is more likely to be attacked, having different security vulnerabilities. The firmware is outdated and not updated against current attacks anymore.

- Misconfiguration of the endpoints – misconfigurations

Misconfiguration can be none or less in place security (ACL, firewall), open and non-secured network ports, using default accounts, old firmware and expired vendor certificates. An example of misconfiguration is also to treat all endpoints as authenticated or put all endpoints on the gatekeeper of only one zone. Using different timers, such as having a SIP register refresh (authentication expiration) time of 30 minutes instead of 15, or a ring no answer duration of two seconds (very short) can lead to endpoint registration problems and un-registration.

Heartbleed bug (serious vulnerability in the popular OpenSSL cryptographic software library):

*"**CVE-2014-0160** is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE [12]. Due to co-incident discovery a duplicate CVE, CVE-2014-0346, which was assigned to us, should not be used, since others independently went public with the CVE-2014-0160 identifier [13]."*

Shellshock (software bug):

"A security flaw in software used by as many as 500m machines around the world is already being used by hackers to carry out a range of attacks, warn experts. Hackers are already taking advantage of the 'Shellshock' flaw, which security researchers warn could be more serious than the Heartbleed security hole and have a dangerous fallout lasting for several years.

The Zscaler ThreatLabZ research team said this morning that it had spotted attacks using the flaw "within hours of the public disclosure". Hackers have been gaining access to *machines using the hole and using it to install additional malware that then leaves them wide open to abuse.*

The researchers gave details of one attack where an Apache web server was tricked into installing malware that gave hackers the ability to open a backdoor connection for remote access, perform Denial of Service attacks or collect sensitive information. Similar Apache software to that targeted in the

attack is estimated to serve around 54.2 per cent of all websites around the world. We rate the severity of this vulnerability to be as critical as that of Heartbleed

vulnerability discovered earlier this year, said the company's Deepen Desai in a blog post. Cloudflare's John Graham-Cumming told The Verge that he too had seen evidence of attacks in the wild: We've seen attackers trying to grab password files, download malware onto machines, get remote access, and more. There was even one attack that involved opening or closing a server's CD / DVD drive. The vulnerability has been hiding in plain sight in the Bash command shell since it was first created in 1989. Bash is included in various Linux distributions and Apple's Mac OS X, which is itself based on Unix. It can be used by the person using the PC to run various commands but is also run invisibly in the background by many software packages. A problem with the way it accepts variables when loaded by these other programs could allow hackers to run malicious code on a victim's computer. Experts warn that it is dangerous because it enables attackers to run powerful commands without permission, potentially leaving victims open to ID theft or loss of sensitive data, but also because it is a simple attack to make which does not require a particularly high level of technical knowledge. Because Bash is widely used in a range of smaller devices, the flaw could also affect various internet-connected hardware, such as CCTV cameras, thermostats and sensors. Although few computer users run Linux on their home desktops, the operating system is used extensively in servers and other hardware, including the machines which host and run websites. It will even affect some Android smartphones, as the Google operating system is also based on Linux [14]."

- DNS non-availability due to dependency on public Internet reachable DNS servers – DNS problems

When an endpoint uses Internet reachable DNS servers instead of internal DNS servers with a DNS name used to register an endpoint to the gatekeeper, they are prone to un-registration or registration rejected problems. There are two kinds of company DNS servers. These are internal DNS servers having a LAN IP address, and external DNS servers, having a WAN IP address. Depending on the type of endpoint (Reachable on LAN, Behind Firewall, Reachable from Public Internet), the correct (internal or external) DNS server is chosen. It is also a good idea to have redundancy in the DNS configuration (two to three servers).

- Insider attacks – insiders

It is not advisable to have Internet reachable endpoints with open SIP ports, as they are likely to be affected from SIP toll-fraud attacks. A better idea is to put them on a public VPN or configure a NAT address to connect to the gatekeepers. Steady patching of endpoints to the latest firmware is also highly advised. Newer firmware releases tackle bugs as well as security holes.

- Non-secure generated public keys – non secure private keys

"An astonishing four out of every 1,000 public keys protecting webmail, online banking, and other sensitive online services provide no cryptographic security, a team of mathematicians has found. The research is the latest to reveal limitations in the tech used by more than a million Internet sites to prevent eavesdropping.

The finding, reported in a paper [15] submitted to a cryptography conference in August, is based on the analysis of some 7.1 million 1024-bit RSA keys published online. By subjecting what's known as the "modulus" of each public key to an algorithm first postulated more than 2,000 years ago by the Greek mathematician Euclid, the researchers looked for underlying factors that were used more than once.

Almost 27,000 of the keys they examined were cryptographically worthless because one of the factors used to generate them was used by at least one other key.

The research is the latest to show the limitations of cryptographic systems that websites use to secure communications. In September, researchers unveiled an attack that silently decoded encrypted traffic [16] as it passed between SSL-protected websites and a Web browser. Over the past few years, the much more standard way of defeating SSL has been to compromise one of the 600 or so entities authorized to mint certificates [17] that are trusted by Firefox and other standard browsers. Given the success and ease of that method, the techniques laid out in the research paper would likely not be an attacker's first choice of exploitation [18]."

- DTF (Dial Through Fraud) attacks – DTF attacks

"Here is a video describing a Dial Through Fraud (DTF) attack. DTF is a form of toll fraud, there the attacker dials into a compromised PBX, gains dial tone, and then dials a

new destination, usually an international number. They "hairpin" though the PBX. The destination is often a premium number and the attacker is using the compromised PBX as a way of generating traffic and revenue [19].

This attack is interesting because it shows how inbound call or robocall generation can be used for DTF and toll fraud. First someone compromises an IP PBX so that an external user can dial in, get dial tone, and dial to an international premium number. Once this access is gained, the attackers can use it at any time for DTF themselves or sell it to an attacker who wants to generate the actual fraud.

Most people think of DTF as being the case there the access to the compromised PBX is sold to many individuals who use it to make international calls, say to talk to relatives in their native countries. This still occurs, but by far the more common attack is to automatically generate inbound calls to the compromised PBX, which hairpin into outbound international calls to the premium numbers, thereby generating a lot of traffic and revenue. This really isn't much different than automated call pumping or Telephony Denial of Service (TDoS) attacks. The attacker sets up an automated call generation operation, probably using Asterisk, a call generator, and SIP trunks. They build an audio file that pauses, enters a code to get dial tone, enters the desired international destination number, and then just keep the call up for some period of time. They run the attack and call a number for the compromised PBX that will give them dial tone. They probably spoof their calling number. The calls are kept up as long as practical, but keeping the calls shorter and/or variable length can make the attack a little less likely to be detected. The calls will usually be generated overnight and/or on the weekend to avoid attention.

If you watch the video, this is what happened. The attacker generated the calls at night and the victim had a ton of calls, all to Somalia start up at the exact same time. The calls continued for about 5 hours, at which time the victim noticed the attack. They happened to be an organization that takes calls at night, so they noticed the attack.

As with any DTF or toll fraud attack, paying for the fraud is the responsibility of the enterprise [20].”

- MITM (Man-in-the-Middle) attack and toll-fraud attack – MITM and toll-fraud attacks

A good example of a MITM attack is eavesdropping used by ARP poisoning. Interception and manipulation of data is thus possible. The (voice/video) data consists of signaling traffic (SIP, H.323) and media data (RTP, SRTP). It is advisable to secure both, but the media traffic is more important.

- Other well-known attacks

Further attacks include, but are not limited to, social engineering, phone phreaking, password guessing, brute-force attacks, SPIT (Spam over Internet telephony), voicemail malfunctioning and voice pharming.

Cybercrime is rising and company voice and video infrastructure can be compromised. It can be used by a hacker as a door to step into a company network to gain sensitive data for cyber espionage or sabotage or harm an economical opponent. Nowadays, it is easier to break and steal into a company online, instead of physically breaking and entering the company.

Social engineering attacks play an important role to gain physical access to network devices gathering useful information. This can be used to carry out the initial steps in an attack process. Often, combinations of attacks are used and not single ones. This is done due to obscurity.

TABLE I.

Threat	**Confidentiality**	**Integrity**	**Availability**	**Privacy**
Open SIP ports	x	x		x
Expired certificates		x	x	
Private key forgery	x	x	x	x
DDOS attacks	x	x	x	x
Ghost calls	x	x	x	x
Outdated technology	x	x	x	
Misconfiguration	x	x	x	x
DNS problems			x	
Insider attacks	x	x	x	x
Non-secure private keys	x	x		x
DTF attack	x	x	x	x
MITM and toll-fraud attacks	x	x	x	x
Sum of instances	10 of 12	11 of 12	10 of 12	9 of 12

Table 1: Mapping of threats to CIAP and sum of instances

Tab. 1 gives an overview of the mappings between the different VoIP and Video threats and the security values CIAP (Confidentiality, Integrity, Availability and Privacy). Integrity is the most affected of these values, with confidentiality and availability on the second place, and privacy on the fourth place. Privacy concerns protecting data of individuals, while confidentiality assures that information is not disclosed to unauthorized persons, processes, or devices.

IV. DEFENSE MECHANISMS

The SBC is acting as a voice aware firewall in the audio setup. Also the separation of data and voice using VLAN (Virtual Local Area Network) technology is very important for security reasons. An encrypted connection, using latest encryption and hashing algorithms, between the central infrastructure components and remote offices is necessary due to data integrity.

The use of soft-phones holds an additional threat vector, as attackers might get access to a compromised PC and thus get further access to the enterprise network and do harm.

On the video side, there must be credentials for each device (passwords for their zone). The proposal is to use the MCU chassis with conductor to provide security in Video meeting spots (configured on the MCU) with a MCU bridge allocated to WebEx enabled Telepresence meetings and CMR (Collaboration Meeting Rooms) hybrid. These meeting rooms are PIN protected and easily extended to many employees, each with individual SIP URI address, as resources are coming from the cloud.

As can be seen in Fig. 2 it is crucial to separate the different security layers and zones by DMZ (Demilitarized Zone) technology using firewalls. A thorough firewall security concept must be in place to run a company video infrastructure. The security concept must be approved by the company's internal security department.

The following countermeasures against threats are helpful in enterprise networks:

- OS hardening and OS patching of all different OS – OS hardening and patching

It is important to secure Internet reachable SIP ports on devices with access-lists and trust-lists. Also to have firewalls and a thorough security concept.

- Firmware upgrading of endpoints and infrastructure to the latest stable software releases – firmware upgrades

Staying on the latest firmware releases is necessary for a company to remain safe. It is time consuming, dependent on the number of endpoints to patch and can be outsourced to the company's service provider, if necessary.

- First test and verify changes and upgrades in a lab environment, before they go into production – test and verification of changes and upgrades

Always test new functionalities, new firmware versions for endpoints or software releases for infrastructure equipment first in a test lab. The interoperability and stability of a network is core for a service provider to reach an availability of 99.85 % at least. This comes down to about 1 hour downtime per month.

- Avoiding using non-secure protocols, like FTP or HTTP – not using non-secure protocols

As recommendation from the SOC (Security Operation Center), the use of non-secure protocols like HTTP, Telnet or FTP is forbidden within the company. It is much better to use secure protocols like HTTPS, SSH and SFTP.

- Using encryption, authentication, secure protocols (SIP, SRTP, TLS) and NAT – using encryption, authentication and secure protocols

Do not treat every source as authenticated on the gatekeepers, where the registration of endpoints takes place. As companies transmit sensitive data within the network and also with other companies, partners or customers, this data (voice and video) must be encrypted and thus secured.

- Security concept for enterprise IT infrastructure – enterprise security concept

A company can install SecAst (www.generationd.com) for a PBX to trap and block hackers who have somehow gained access to credentials - and then block them. They key is to at least know you are under attack so you can dig deeper to find out why.

- Replacing old, non-patched, non-secure hardware (ISDN gateway) – replacing outdated hardware

Outdated hardware should be replaced and virtualized, if possible. Reasons are end of support, end of life and redundancy reasons.

- Accurate documentation of infrastructure and up-to-date operational procedures in place – documentation and OPROCS

Accurate documentation is important for incidents, problems and change management support records according to ITIL, version 3. OPROCS (operating procedures) are central to a structured and effective way of working.

In general, the threats against VoIP and Video enterprise networks are aimed against the following values (also named security risks): confidentiality, integrity, availability and privacy. The targets of the attacks are infrastructure devices, security devices, network services, endpoints and infrastructure. In this paper we concentrate on endpoints and infrastructure, namely in the context of voice and video.

A lot of these attacks are network based attacks, so a good network status must be maintained. This can be assured by the use of anti-virus software on clients, use of NAC (Network Access Control) on network ports. Additionally as firewalls and IDS/IPS (Intrusion Detection System, Intrusion Prevention System) technology, doing regular security scans against common and new vulnerabilities.

Further defense mechanisms compromise a company-wide security policy as well as security training and processes in place. Best practices, like this paper, are fundamental for the formal statements of the rules of a security policy, to which employee have to comply. A key aspect of every security policy is the assets (network devices, etc.) to be secured. Risks and costs are evaluated. Risk is minimized by placing rules, standard guidelines for working, and inter-connection to secure data and assets. It can be further calculated with an index using the following parameters: severity, probability, control range and risk index. The risk index is calculated as severity multiplied with probability and the result is divided by the control range, Also the processes and procedures for managing incidents are described in a security policy. Continuous security is assured by the policy life cycle: secure, monitor, test and improve. Some companies even need to deploy higher security mechanisms as they have to comply with regulations of data processing, such as PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes Oxley) or HIPAA (Health Insurance Portability and Accountability Act). This is dependent on the company branch and the geographical residence of the company. Trust and Identity management servers add additional security. An example is the use of the TACACS protocol to authenticate with a domain user against a network device. A further example is the enablement of ACL (Access Control Lists), SNMP (Simple Network Management Protocol), NTP (Network Time Protocol) and Syslog on network devices for monitoring purposes. NTP is important to have accurate time and date on log entries, which can be the further analyzed.

It is important for a company to stay within the above mentioned regulations, because otherwise no job competition would be possible. We further propose to use a hybrid approach, a combination of technical defense mechanisms as well as organizational training and processes. With technical measures alone, it has been proven many times that they are not sufficient to combat the ever changing novel attacks carried out.

TABLE 2

Defense Mechanism	**Confidentiality**	**Integrity**	**Availability**	**Privacy**
OS hardening and patching	x	x	x	x
Firmware upgrades	x	x	x	
Test and verification of changes and upgrades	x	x	x	
Not using non-secure protocols	x	x	x	x
Using encryption, authentication and secure protocols	x	x	x	x
Enterprise security concept	x	x	x	x
Replacing outdated hardware	x	x	x	
Documentation and OPROCS	x	x	x	
Sum of instances	8 of 8	8 of 8	8 of 8	4 of 8

Table 2: Mapping of defense mechanism to CIAP and sum of instances

In Tab. 2 it can be easily seen that the defense mechanism are very well aimed at the security values of confidentiality, integrity and availability. The privacy point can be improved in the proposed defense system architecture.

V. RELATED WORK

Shin et al. [7] present a flexible greylisting approach for Spam over Internet Telephony (SPIT) detection. In this approach the system decides, whether the call will be connected or blocked. The system uses a Bayesian network to make filter decisions.

Quittek et al. [8] analyse human communication patterns in VoIP calls and derived Turing tests in order to prevent SPIT.

d'Heureuse et al. [3] present a framework to protect SIP based infrastructures. The framework is protecting against SPIT using only black-, and whitelists. Their heavyweight approach is placed at three different locations in the operator's network, the SBC, Application Server (AS) and IP phone.

Tartarelli et al. [9] describe how information is stored in different types of call data records and how to check the sanity of telecommunication data stored in these. The authors also propose methods to aggregate the data to reduce the amount of data. This work can complement our own.

Fernandez et al. [10] design several UML models of some aspects of VoIP infrastructure, including architectures and basic use cases.

The authors also present security patterns that describe countermeasures to VoIP attacks, which can nicely complement our work. Nevertheless, Fernandez et al. do not propose to build a system.

Keromytis [4],[5],[6] presents a survey of VoIP threats based on published common vulnerability enumerations and publications in the field. Ehlert [1] and Ryan [2] present surveys with regard to denial-of-service attacks for VoIP systems.

None of the aforementioned approaches considers a light weight best practice approach for VoIP security. Sorge et al. [11] investigate the legal issues involved with call filtering solutions. The authors describe the legal situation for the US and the German legal system. Sorge et al. have investigated the problem in general and have led the foundation for more system specific work.

VI. CONCLUSIONS AND FUTURE WORK

We showed a Voice-over-IP and Video-over-IP threat analysis from a practitioner's viewpoint and presented some solutions to counteract these threats. The results of our work can be applied to existing VoIP systems with little effort.

The developed approach offers the following main benefits:

- A structured overview of current VoIP threats
- Systematic identification of relevant threats and cost effective countermeasures
- Improving the security of existing VoIP and Video communication systems by adding security to prevent common attacks
- Supports the integration of security measures for common enterprise architectures of VoIP systems

Future work will focus on an automated threat detection system, specifically engineered for common VoIP and Video enterprise architectures. The system will rely mostly on existing and common software tools in such systems. One of the major issues with VoIP and video technology however still is that in spite of being widely deployed it is not very well protected. And this is where we need to put an ongoing focus.

REFERENCES

[1] Sven Ehlert, Dimitris Geneiatakis, Thomas Magedanz, Survey of network security systems to counter SIP-based denial-of-service attacks, Computers & Security, Volume 29, Issue 2, 2010, 225-243

[2] Ryan Farley, Xinyuan Wang, Exploiting VoIP softphone vulnerabilities to disable host computers: Attacks and mitigation, International Journal of Critical Infrastructure Protection, Volume 7, Issue 3, 2014, 141-154

[3] d'Heureuse N, Seedorf J, Niccolini S, Ewald T. Protecting sip-based networks and services from unwanted communications. GLOBECOM, IEEE, 2008; 1–5.

[4] Angelos D. Keromytis. A Survey of Voice over IP Security Research. In Proceedings of the 5th International Conference on Information Systems Security (ICISS '09), Atul Prakash and Indranil Sen Gupta (Eds.). Springer-Verlag, Berlin, Heidelberg, 2009, 1-17.

[5] Angelos D. Keromytis, "Voice-over-IP Security: Research and Practice," IEEE Security & Privacy, vol. 8, no. 2, pp. 76-78

[6] Angelos D. Keromytis. Voice over IP: Risks, Threats and Vulnerabilities. In: Proceedings of the Cyber Infrastructure Protection (CIP) Conference, 2009, 223-240

[7] Shin D, Ahn J, Shim C. Progressive multi gray- leveling: A voice spam protection algorithm. IEEE Network 2006; 9(1):18–24.

[8] Quittek J, Niccolini S, Tartarelli S, Stiemerling M, Brunner M, Ewald T. Detecting spit calls by checking human communication patterns. ARES 2007 Proceedings, IEEE, 2007; 1–6.

[9] Tartarelli S, d'Heureuse N, Niccolini S. Lessons learned on the usage of call logs for security and management in ip telephony. Communications Magazine, IEEE 2010; 48(12):76 –82.

[10] Fernandez EB, Pelaez JC, Larrondo-Petrie MM. Security patterns for voice over ip networks. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, IEEE Computer Society: Washington, DC, USA, 2007; 19–29.

[11] Sorge C, Niccolini S, Seedorf J. The legal ramifications of call-filtering solutions. IEEE Security and Privacy 2010; 8:45–50

[12] http://cve.mitre.org

[13] http://heartbleed.com/

[14] http://www.telegraph.co.uk/technology/internet-security/11123096/Hackers-already-using-Shellshock-bug-to-attack-victims.html

[15] http://eprint.iacr.org/2012/064.pdf

[16] http://arstechnica.com/business/2011/09/new-javascript-hacking-tool-can-intercept-paypal-other-secure-sessions/

[17] http://arstechnica.com/security/2011/08/earlier-this-year-an-iranian/

[18] http://arstechnica.com/business/2012/02/crypto-shocker-four-of-every-1000-public-keys-provide-no-security/

[19] http://www.bbc.co.uk/programmes/p017fb0c

[20]http://voipsecurityblog.typepad.com/marks_voip_security_blog/2013/04/dial-through-fraud-dtftoll-fraud-attack-using-robocalls.html